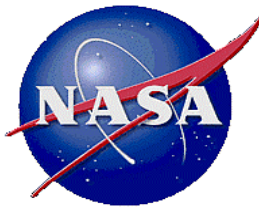


Integration of Technical Risk Management with Decision Analysis

Presented at NASA Project Management Challenge 2007 Conference

Galveston, Texas

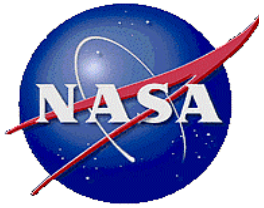
February 6-7, 2007

Homayoon Dezfuli, Ph.D., NASA HQ *(hdezfuli@nasa.gov)*
Robert Youngblood, Ph.D., ISL, Inc. *(ryoungblood@islinc.com)*

Acknowledgement

- Some of the materials in this presentation are based on methodology developed by the Office of Safety and Mission assurance in support of the following activities:
  - Revision of NASA requirements for system safety (NPR 8715.3A dated September 12, 2006)
  - Revision of NASA System Engineering Handbook (to be released June 2007)
  - Development of a new NASA standard entitled “Risk-informed Management of Safety and Mission Success” (planned for release before the end of fiscal year 2007)

Why Integrate Technical Risk Management with Decision Analysis?



Excerpt from 2006 Third Quarterly Aerospace Safety Advisory Panel (ASAP) Report

"*With regards to risk assessments that are being made to support launch decisions, it appears that a series of fragmented, non standardized tools and methodologies are in use. The result is that risk recommendations to senior management concerning individual hazards effecting launch are sometimes made in isolation without consideration of overall launch risk. For example, the most recent Shuttle launch focused heavily on two of the 569 potentially catastrophic hazards currently known to exist, without any assessment of the overall likelihood of such a catastrophic failure. A lack of confidence in the technical basis for the assessments also appears to sometimes exist and variations in risk matrix definitions among programs has been observed. Lastly, only limited guidance is available concerning agency policies on what risks should be accepted under what conditions. The ASAP recommends that a comprehensive risk assessment, communication and acceptance process be implemented to ensure that overall launch risk is considered in an integrated and consistent manner. The process should be sound, mature, consistently implemented to yield high confidence and consistent results that are generally accepted by the majority of the community.*"

Key Points

- **Decision analysis can be a powerful tool for aligning decisions with program objectives, given the current state of knowledge and the decision-maker's preferences**
- **Modern risk analysis methodology can significantly improve on the one-at-a-time management of risk issues criticized by the ASAP report**
- **Therefore:**
  - **Perform Technical Risk Management within a decision analysis framework**
  - **Use modern risk analysis methodology, including probabilistic risk assessment (PRA)**
  - **Retain the track, control, and accountability strengths of the Continuous Risk Management (CRM) Process**

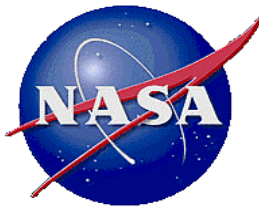
Outline

- Background
- State of Practice of Risk Management (RM) at NASA
- An Example of How Risks are Handled in Decision Processes
- Need for a More Rigorous Approach to Inform Risk Management Decisions
- An Analytical Framework to Inform Risk Management Decisions
- The Role of Probabilistic Risk Assessment (PRA) in Risk Management
- PRA Methodology Synopsis
- Summary

Background

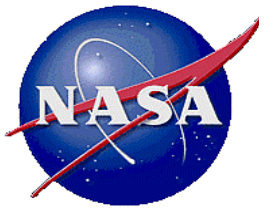
- NASA is embarking on a comprehensive space exploration program
- The goals of the exploration program are "*safe, sustained, affordable human and robotic exploration of the Moon, Mars, and beyond ... for less than one percent of the federal budget*"
- Meeting these goals requires development of a constellation of new systems
- The design and development of these systems will involve many decisions that require weighting/trading various competing programmatic and technical considerations against one another

Programmatic and Technical Considerations that Should be Factored into Our Decisions

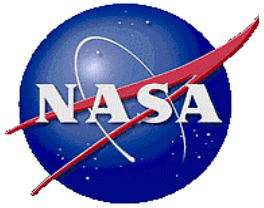


- **Affordability**
  - Meet budget constraints related to design and development cost, technology development cost, operation cost, and facility cost
- **Mission Technical Objectives and Performance**
  - Accomplish technical objectives in a sustainable manner and on schedule
  - Enhance effectiveness and performance
- **Safety**
  - Protect the health of public and workforce, the environment and mission assets
- **Stakeholder Expectations**
  - Meet needs of intra-agency and extra-agency stakeholders

The Role of Risk Management



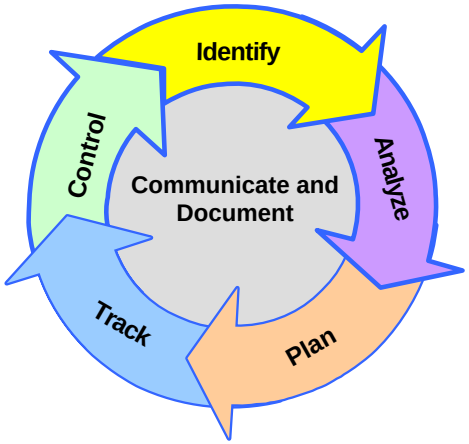
- **Purpose of risk management is to promote program success**
  - **Incorporating risk-informed decisionmaking in the design and formulation of the program baseline**
  - **Proactive identification and control of departures from the program baseline**
- **An effective and proactive RM process should**
  - **Provide input to determine the preferred decision alternative in light of programmatic objectives**
  - **Assess risk associated with implementation of the selected alternative**
  - **Assist in setting resource priorities (including prioritization of work to resolve uncertainties if warranted)**
  - **Plan, track, and control risk during the implementation of the selected alternative**
  - **Iterate with previous steps in light of new information**



State of Practice of Risk Management at NASA

Continuous Risk Management (CRM) Process

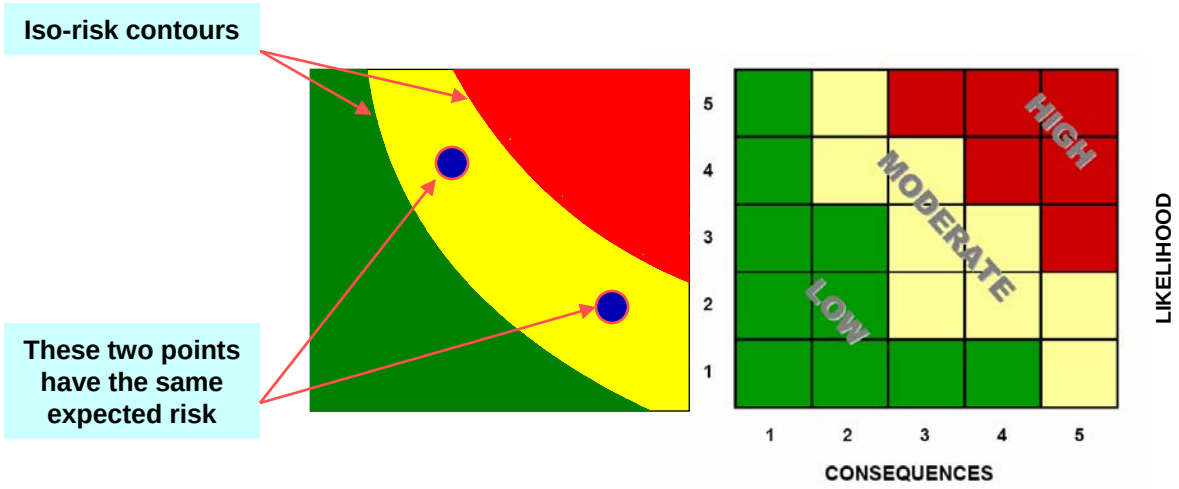
- Identify – *Identify* program risk "issues"
- Analyze – Estimate the likelihood and consequence components of the risk issues
- Plan – *Plan* the *Track* and *Control* actions
- Track – *Track* and compile the necessary risk data, measuring how the CRM process is progressing
- Control – Determine the appropriate *Control* action, execute the decision linked to that action, and verify its effectiveness
- Communicate and Document – communicating and documenting all risk information throughout each program phase



Current emphasis on

- **"management" of individual "risks," given a decision already made somewhere else**
- **monitoring and accountability for action items associated with "risks"**

Risk Matrix Paradigm



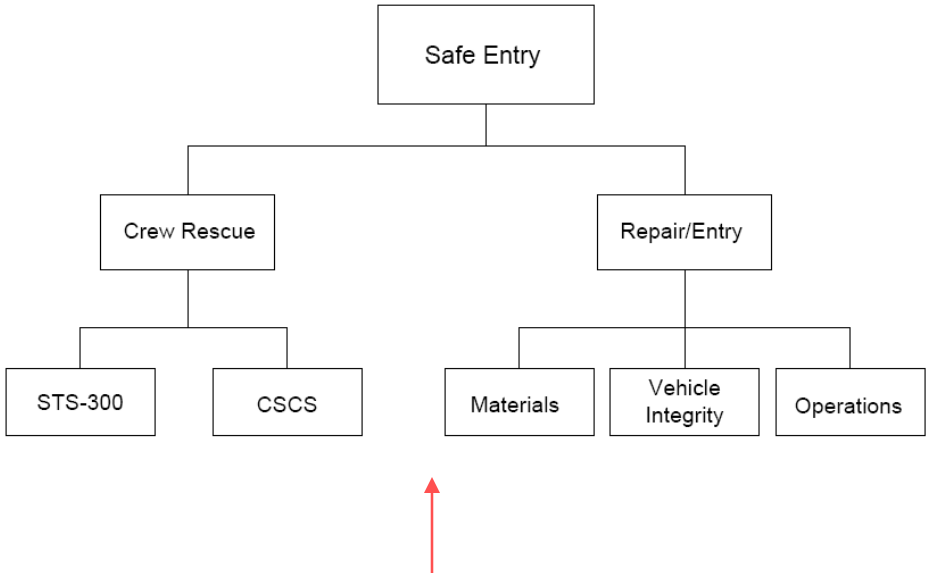
- Risk "issues" are mapped onto the matrix individually
  - Interaction between risks is not considered
  - Total risk from all "issues" is not evaluated
  - Highly subjective; uncertainties are not formally accounted for
  - Unsuitable for combining risks to obtain aggregate risk
- Risk tolerance boundaries are defined based on iso-risk contours
  - Expected consequences (probability times consequences) do not adequately inform decisions relating to safety
- Limited ability to support risk-trade studies

An Example of How Risks are Handled in Decision Processes

STS-121 (OV-103 Discovery) Contingency Planning

Decision Alternatives

1. **Crew Rescue:**
   - Success of contingency (rescue) flight (STS-300)
   - Success of Contingency Shuttle Crew Support (CSCS) capability (on-orbit safe haven)
2. **Repair/Entry:**
   - Successful application of patching materials (STA-54) to repair damaged heat shield
   - Vehicle integrity during reentry (no downstream heating damage)
   - Successful approach and landing (operations)



Source of Figure: Shuttle Program, NASA-JSC

Pros and Cons Associated with Decision Alternative 1 *(Data Source: Shuttle Program)*

STS-300

Pros

1. Nominal STS-300 processing supports CSCS capability (M)
   - Potential for Schedule compression
2. Full rescue capability (H)
3. Vehicle within certified limits for ascent/entry (H)

Cons

1. Inability to launch (M)
   - Weather delay
   - System failures
2. Post-launch damage (L)
   - Ascent environment unchanged
3. Post-launch system failures (L)
4. Loss of OV-103 (H)
5. Places additional crew at risk (M)

CSCS

Pros

1. Adequate consumables (44 days O2) to support STS-300 timeline (H)
2. 18P consumables currently not accounted for (M)
3. Expired Russian LiOH available for CO2 removal (L)
4. No increased risk to ISS Subsystems (except ECLSS) (L)

Cons

1. CSCS duration dictated by ISS/SSP consumables and ECLSS hardware availability (M)
   - CDRA represents most significant risk
2. Decreased systems fault tolerance and consumables due to crew load (O2 generation, CO2 removal, food/water, waste recovery) (M)
3. No emergency escape to support Shuttle crewmembers. (M)
4. ISS emergency/contingency EVA impacts consumables (L)
5. ISS may be de-manned after STS-300 (H)

OBSERVATIONS

Adverse consequences of Interest are:

- **Loss of crew**
- **Loss of vehicle (OV-103)**
- **Evacuation of station**

It appears that Low (L), Medium (M), and High (H) are expressions of degree of belief in the truth of the proposition

Pros and Cons Associated with Decision Alternative 2 *(Data Source: Shuttle Program)*

Materials

Pros

1. STA-54 has performed as well as undamaged tiles during ground testing (H)
2. Ground testing has shown acceptable adhesion (H)
3. Hardness exceeds requirements (H)
4. Underfill has been verified to be +/- 1/8" of guideline (H)

Cons

1. STA-54 Uncertified (H)
   - Limited testing
   - Repair math models not validated
2. No arc jet validation of repair (M)
3. 0-G effects on STA-54 are unknown (H)
   - Adhesion
   - Bubbling

Vehicle Integrity

Pros

1. Original factor of safety 1.1 without repair (L)
2. No downstream damage detected (H)
3. Margin of safety maintained on structure and tile (H)
4. Predicted boundary layer transition not expected to be Catastrophic (M)
   - HR ORBI-249 - Hazard Severity: Critical
   - Past flight experience STS-28 & STS-73

Cons

1. Structural margin of safety dependent on STA-54 adhesion (H)
   - Adhesion can't be verified
2. Analytical uncertainty unknown (H)

Operations

Pros

1. Restrictions within current operational capability (M)
   - Reduced structural loads

Cons

1. HAC restrictions may limit landing sites (weather/wind dependent) (L)
2. Sink rate limits (crew/weather dependent) (L)
3. Public risk due to overflight (entry profile/landing site dependent) (L)

OBSERVATIONS

- **Additional adverse consequence of interest: Public death or injury**
- **Acknowledgment of uncertainties (imperfect models and a limited state of knowledge)**

Which Decision Alternative is More Desirable?

Crew Rescue

Probable			
Infrequent			X
Remote			
Improbable			
	Marg.	Crit.	Cat.

Repair/Entry

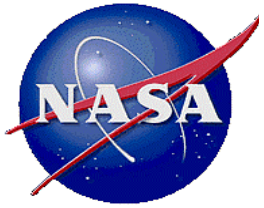
Probable			
Infrequent			X ↓
Remote			
Improbable			
	Marg.	Crit.	Cat.

Source of Matrices: Shuttle Program, NASA-JSC

COMMENTS

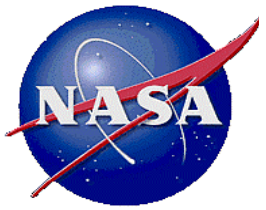
- **The shuttle program uses the above matrix to assign a level of risk to a hazard based on its likelihood and consequence severity**
  - **Catastrophic: hazard could result in a mishap causing fatal injury to personnel and/or loss of one or more major elements of the flight vehicle or ground facility**
  - **Infrequent: Could happen in the life of the program. Controls have significant limitations or uncertainties**
- **The matrix is used here to analyze decisions**
- **The definition of "catastrophic" does not discriminate between human safety and asset safety (defined as an inclusive consequence severity level)**

Need for a More Rigorous Approach to Inform Risk Management Decisions



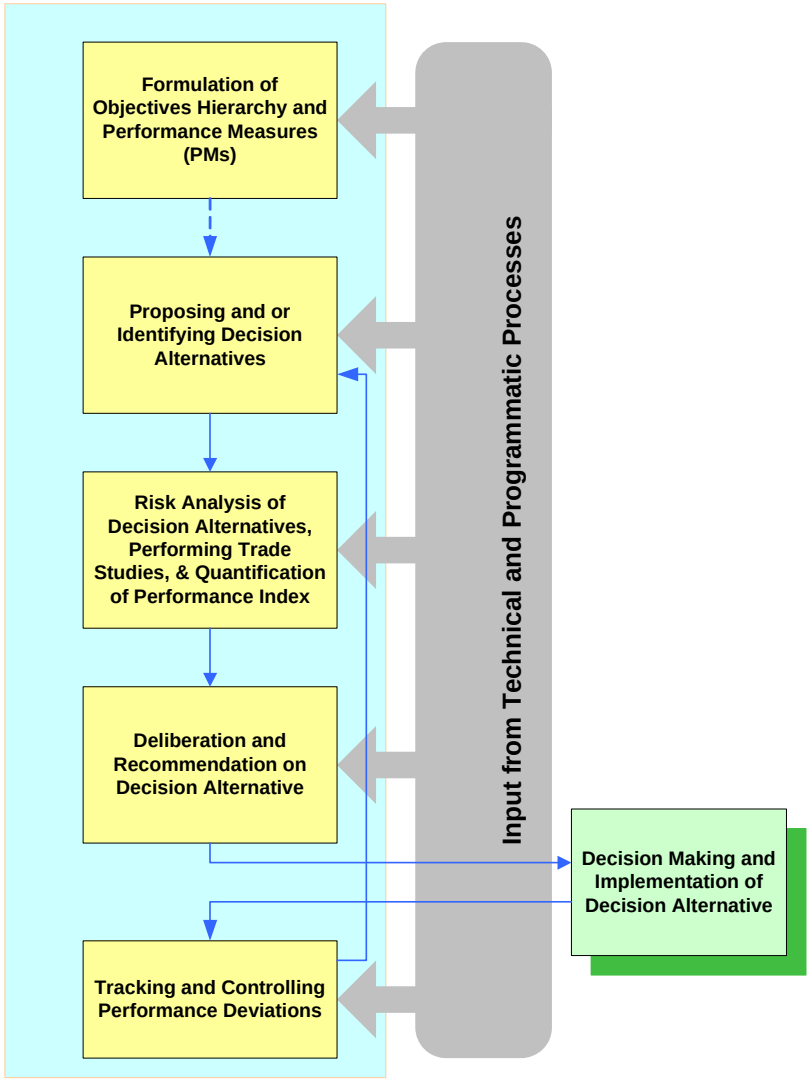
- **Characteristics of our Decision Situations**
  - **They are complex: Need a systematic framework to sort things out**
  - **Must deal with uncertainty: Need to assess uncertainty analytically, know when it is necessary to reduce it**
  - **Must deal with multiple Objectives: Need to employ analytic decision techniques to handle competing priorities (apples vs. oranges)**

An Analytic Framework to Inform Risk Management Decisions

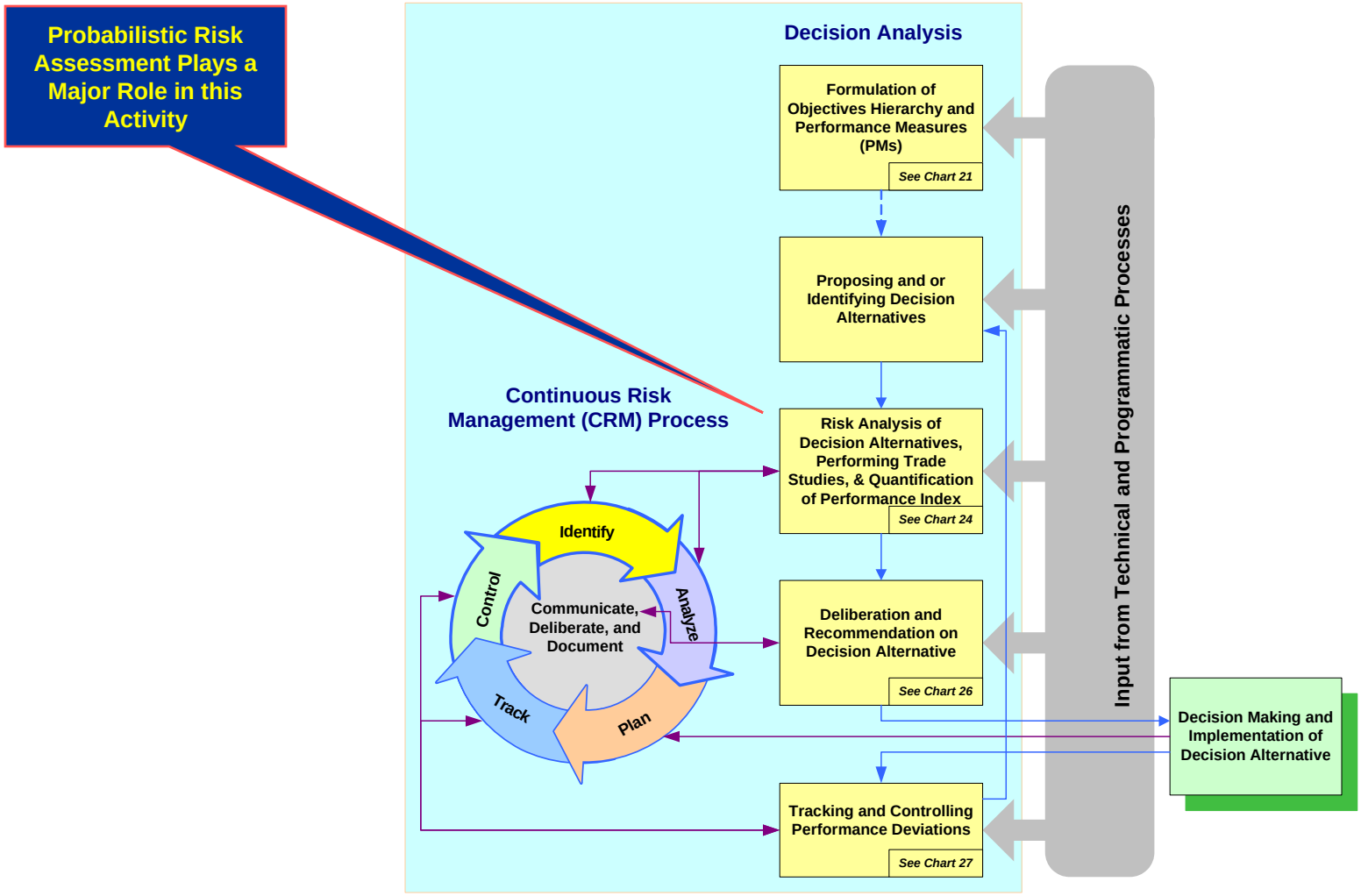


- Model consequences of decision alternatives in terms of impact on fundamental objectives
  - Use performance Measures (PMs) as metrics to characterize performance of the decision alternatives with respect to a particular fundamental objective. Examples:
    - PM for crew safety is the probability of loss of crew
    - PM for space asset safety is the probability of loss of space vehicle
    - PM for public safety is the probability of public death or injury
    - PM for station occupancy is the probability of evacuation
  - Inclusion of uncertainties is critical in evaluating PMs
- Compare the consequences of decision alternatives on the PMs
- Collectively consider all PMs and associated uncertainties to inform risk management decisions (deliberation has an important role here)

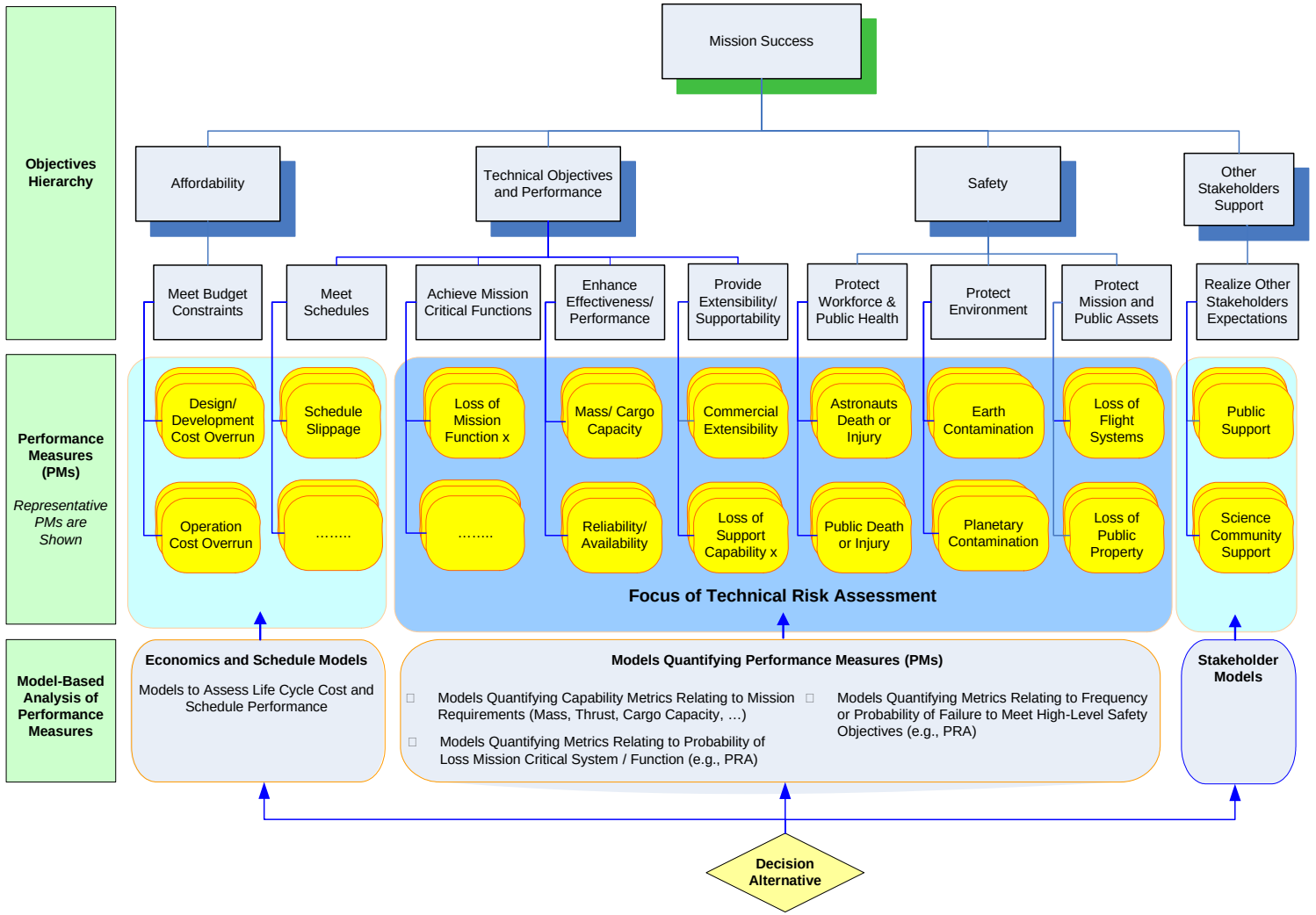
Decision Analysis



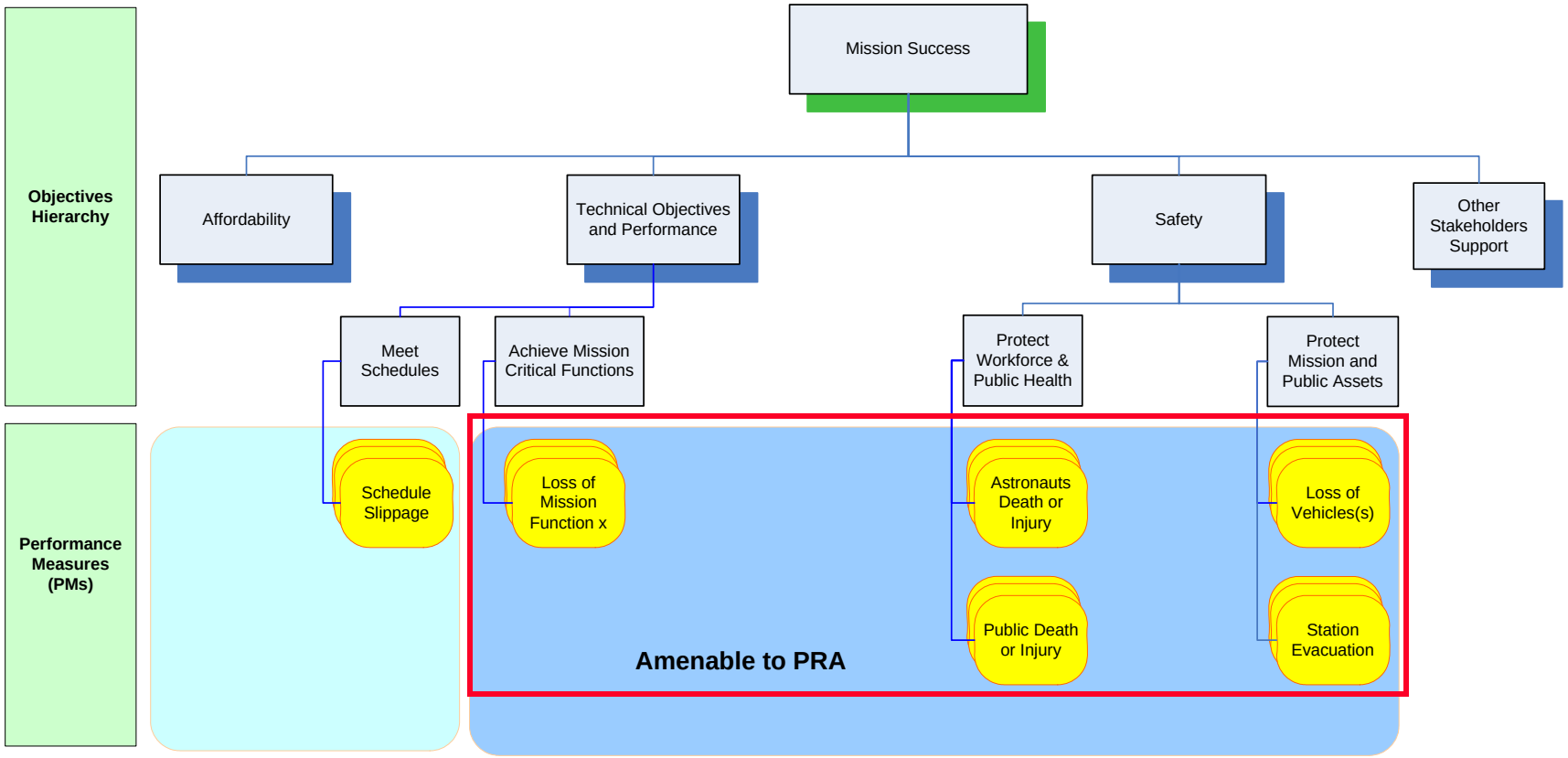
Integration of CRM Process with Decision Analysis



Formulation of Objective Hierarchy and Performance Measures (PMs)



PMs of Interest to the Decision Situation Discussed Earlier



PMs of Interest to NASA's Exploration Systems Architecture Study (ESAS)

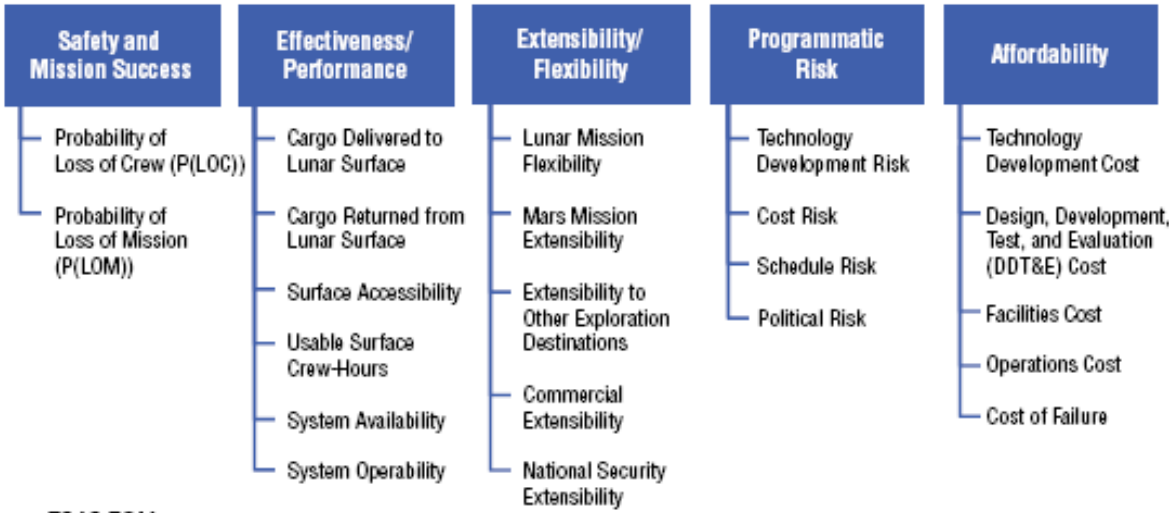


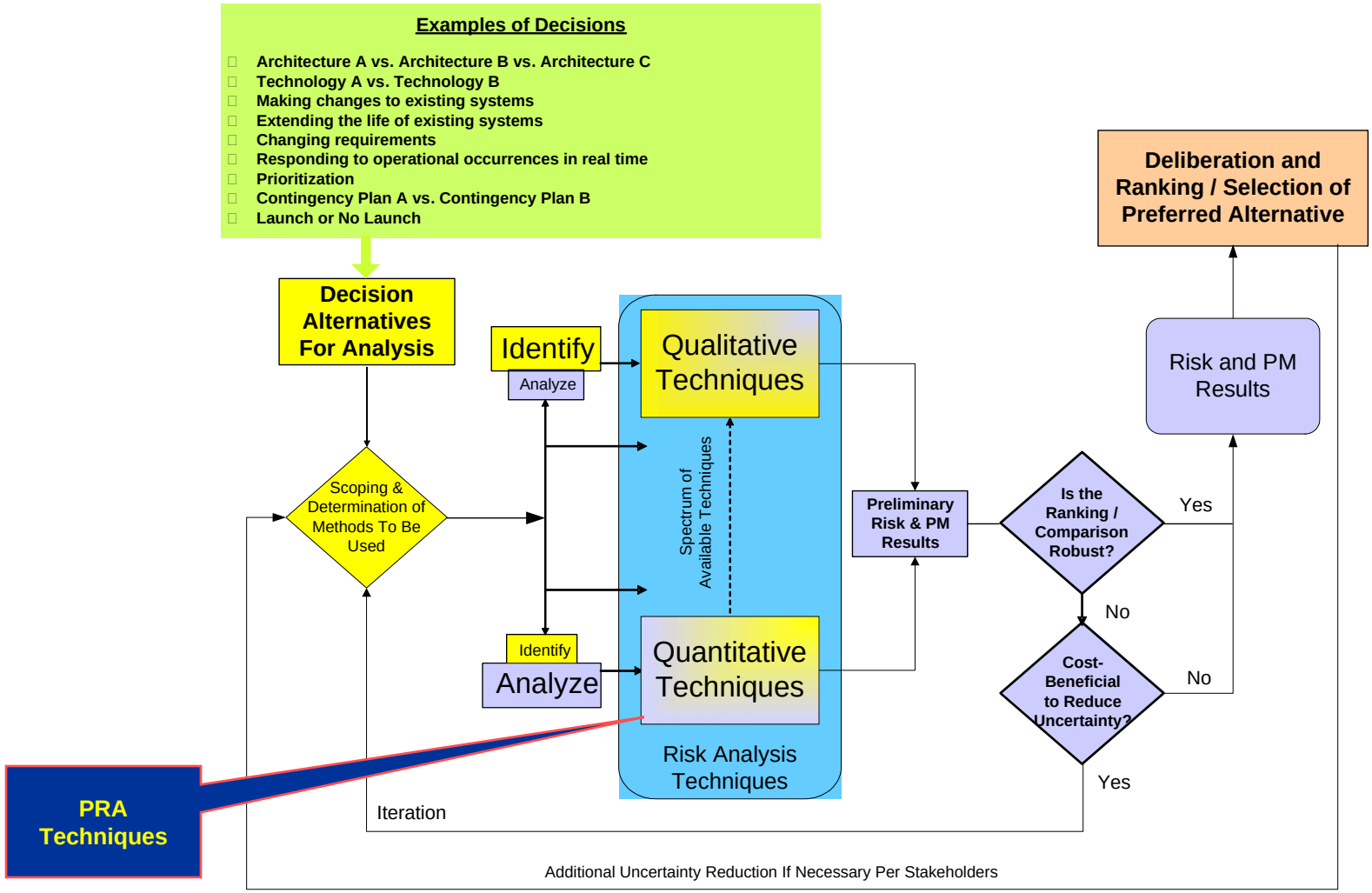
Figure 1-1. ESAS FOMs

In ESAS study, the PMs were referred to as "Figures of Merit (FOMs)"

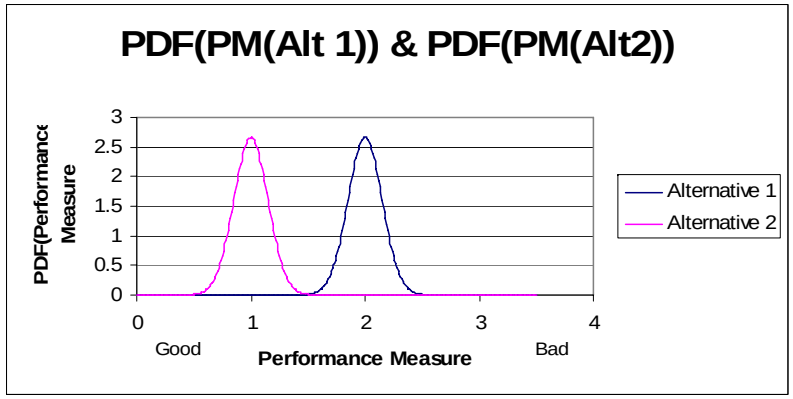
The various trade studies conducted by the ESAS team used a common set of FOMs for evaluation. Each option was quantitatively or qualitatively assessed against the FOMs shown in **Figure 1-1**. FOMs are included in the areas of: safety and mission success, effectiveness and performance, extensibility and flexibility, programmatic risk, and affordability. FOMs were selected to be as mutually independent and measurable as possible. Definitions of each of these FOMs are provided in **Appendix 2D, ESAS FOM Definitions**, together with a list of measurable proxy variables and drivers used to evaluate the impacts of trade study options against the individual FOMs.

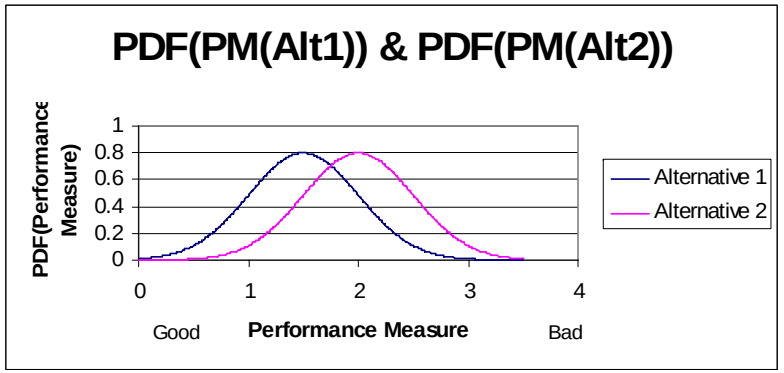
Source: ESAS Report

Risk Analysis of Decision Alternatives



Implications of Uncertainty in Comparing Alternatives





PDF (PM (Alt X)) : Probability Density Function of Performance Measure associated with Decision Alternative X

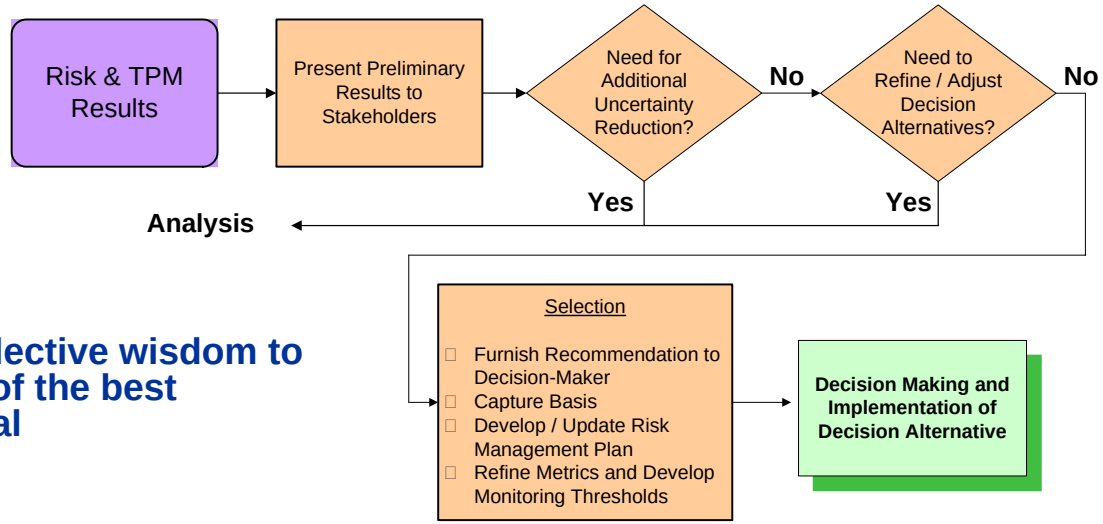
Alt 2 is clearly better than Alt 1

Assuming that the uncertainty distributions reflect the actual state of knowledge, it is very unlikely that uncertainty reduction will improve the decision

Alt 1 is slightly better on average, but uncertainty in performance implies some probability that Alt 2 is actually better than Alt 1

Uncertainty reduction will improve the decision

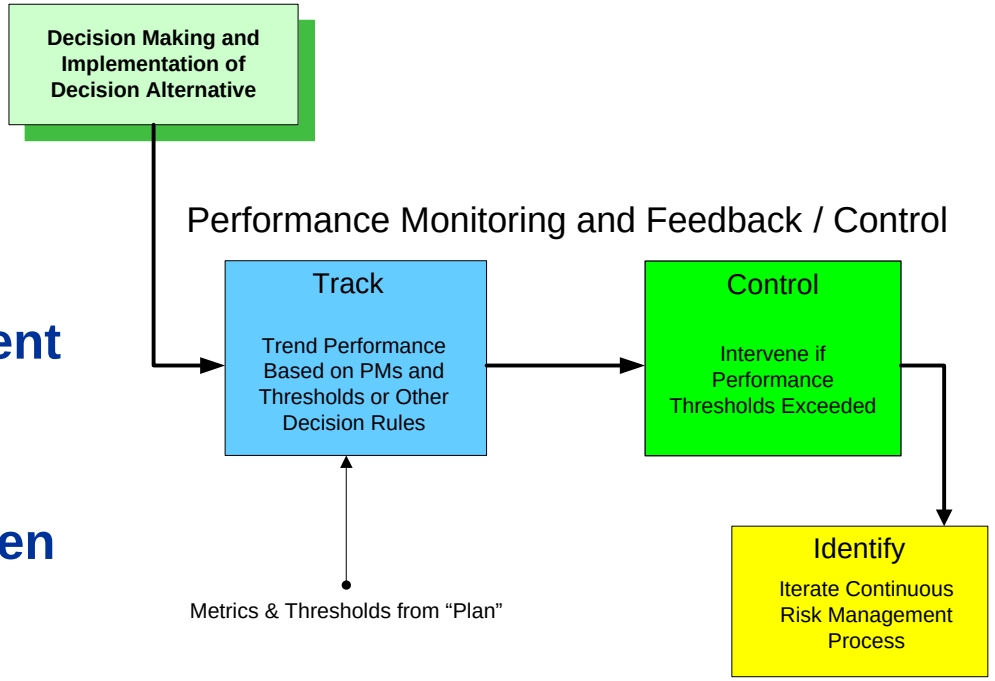
Deliberation and RM Planning



- **Deliberation**
  - To make use of collective wisdom to promote selection of the best alternative for actual implementation
- **RM Planning**
  - Identified and analyzed risks are managed in one of four possible actions (Mitigate, Research, Watch, or Accept)
  - A portfolio of observables and thresholds needs to be identified
    - Measurable (or calculable) parameters
    - provides timely indication of performance issues
  - RM Protocols are determined
  - Responsibility for Tracking activities is assigned

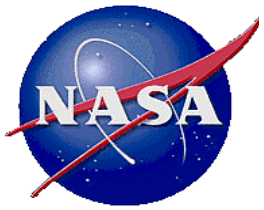
Monitoring Performance Deviations

- **Detection of significant deviations from program intent in a timely fashion, without over-burdening the program**
- **Mitigation/Control of risk when a performance threshold is exceeded**
  - **A perceived insignificant risk "issue" becomes significant**
  - **Emergence of new risk "issues"**



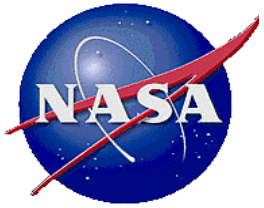
The Role of Probabilistic Risk Assessment (PRA) in Risk Management

PRA can be a Powerful Tool for Risk Management



- Quantifies goal-related performance measures
  - Probability of Loss of Crew (LOC) versus Reliability Analysis of sub-systems
  - PRA metrics are integral risk metrics as opposed to limited metrics such as sub-system reliability
- Captures dependences and other relationships between sub-systems
- Works within a scenario-based concept of risk that best informs decision-making
  - Identifies contributing elements (initiating events, pivotal events, basic events)
  - Quantifies the risk significance of contributing elements, helping focus on where improvements will be effective
  - Provides a means of re-allocating analytical priorities according to where the dominant risk contributors appear to be coming from
  - Provides a framework for a monitoring / trending program to detect risk-significant adverse trends in performance

PRA can be a Powerful Tool for Risk Management (cont.)



- Quantifies uncertainty and ranks contributors to uncertainty
- Supports trade studies by quantifying
  - The most goal-related metrics
  - System interfaces and dependencies
  - Responses to system and function challenges
  - Effects of varying performance levels of different systems

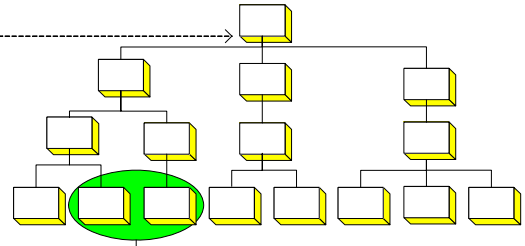
PRA Methodology Synopsis

Understanding of Consequence of Interest (Performance Measures (PMs)) to Decision- maker

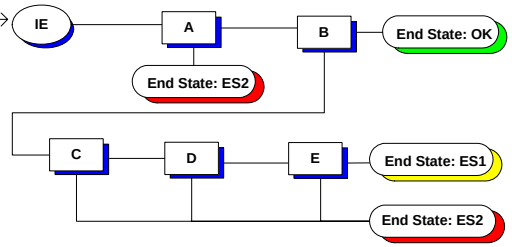
End State: ES1

End State: ES2

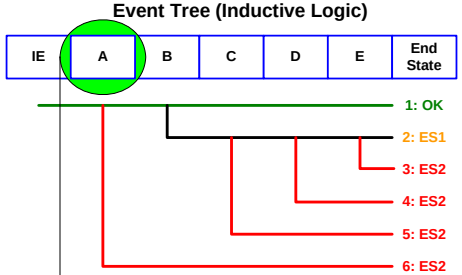
Master Logic Diagram (Hierarchical Structure)



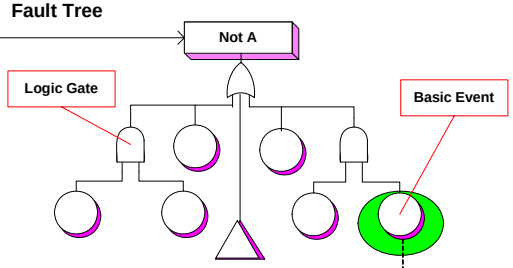
Event Sequence Diagram (Inductive Logic)



Event Tree (Inductive Logic)



Modeling of Pivotal Events Using Techniques such as Fault Tree

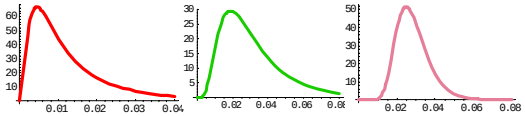


Modeling of Basic Events Using Various Techniques (Some Examples are Shown Below)

$$Q_k^{(m)} = \frac{1}{\binom{m-1}{k-1}} \alpha_k Q_t$$

$$Pr_f(t) = 1 - e^{-\lambda t}$$

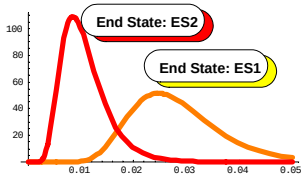
Probabilistic Modeling of Basic Events



Examples:
Probability that the hardware x fails when needed
Probability of nozzle burn-through
Probability of common cause failure of two redundant devices

The uncertainty in occurrence frequency of an event is characterized by a probability distribution

Model Integration and Quantification



Quantification of PMs and propagation of epistemic uncertainties

Communicating Risk Results and Insights to Decision-maker

- Reporting PMs and associated uncertainties
- Ranking of risk scenarios
- Ranking of risk significance contributors (e.g., hardware failure, human errors, etc.)
- Insights into how various systems interact
- Tabulation of key modeling assumptions
- Identification of key contributors to uncertainty
- Proposing candidate risk reduction strategies

Integrated Nature of PRA Addresses Some ASAP Concerns

- Some of the pros and cons of the example discussed earlier would have been modeled explicitly in an integrated risk analysis
- Performance uncertainties are included explicitly
- Treating the issues as consistently as possible, within an integrated framework making use of all available information, is an improvement over mapping each issue separately into a 5x5 and trying to trade them off against each other

Summary

- The proposed RM approach is based on an analytic-deliberative decision-making methodology
- Embeds current Continuous Risk Management (CRM) process in a broader decision analysis framework
- It is analytical because
  - It promotes analyses of the consequences of decision options in terms of PMs relating to program fundamental objectives
  - It promotes the use of analytical methods rather than judgment, wherever the methods are practical
  - It promotes systematic incorporation of decision maker's preferences (values) into decision-alternative ranking process
- It is deliberative because
  - Allows the consideration of elements that have not been captured by the formal analysis
  - Provides an opportunity to scrutinize the modeling assumptions of the analysis and the relevant uncertainties

Acronyms

Alt.	Decision Alternative
Cat.	Catastrophic
CDRA	Carbon Dioxide Removal Assembly
ASAP	Aerospace Safety Advisory Panel
Crit.	Critical
CRM	Continuous Risk Management
CSCS	Contingency Shuttle Crew Support
ECLSS	Environmental Control and Life Support Systems
ESAS	Exploration Systems Architecture Study
EVA	Extravehicular Activity
FOM	Figure of Merit
HAC	Heading Alignment Circle
IE	Initiating Event
ISS	International Space Station
LiOH	Lithium Hydroxide
LOC	Loss of Crew
Marg.	Marginal
PDF	Probability Density Function
PRA	Probabilistic Risk Assessment
PM	Performance Measure
RM	Risk Management
STA-54	Shuttle Tile Ablator 54
STS	Space Transportation System